PROJECT RESULTS

March 2018

MITIGATE

Multidimensional, integrated, risk assessment framework and dynamic, collaborative Risk Management tools for critical information infrastructure

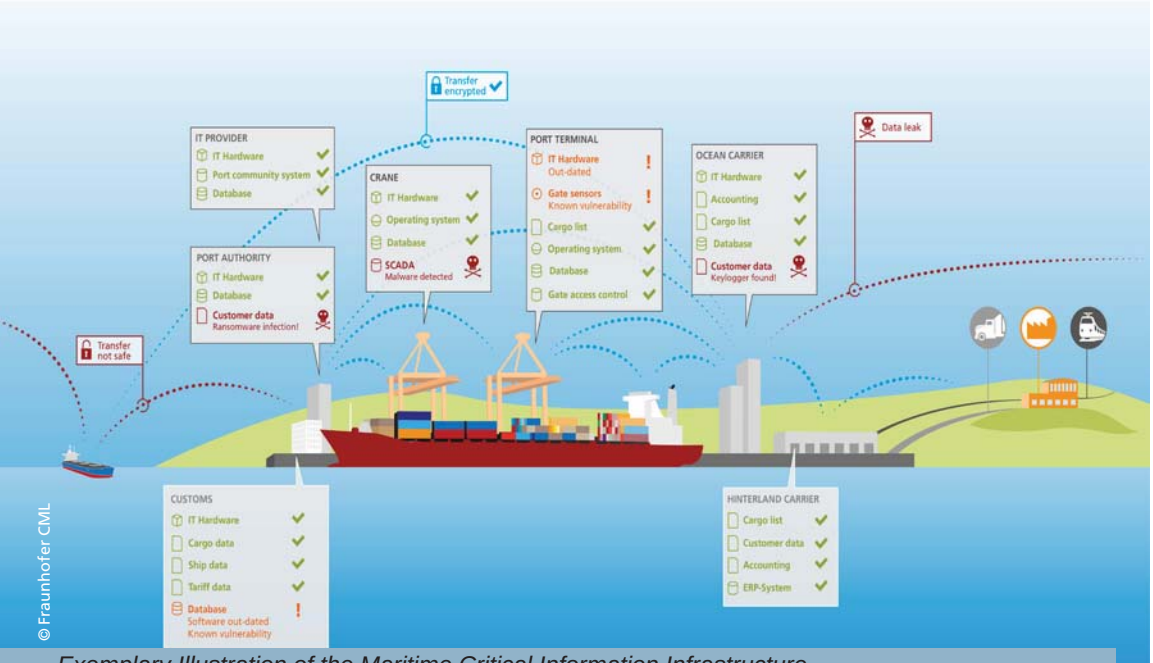
PROTECTING MARITIME SUPPLY CHAIN IT INFRASTRUCTURE

MOTIVATION OF THE MITIGATE PROJECT

Our modern information society depends on functioning and reliable information and communication infrastructures. This fact is being exploited by malicious parties more and more frequently in the recent time. Damages caused by cyber attacks have been on the rise for years. As the supply chain is also a risk chain, companies are increasingly affected by incidents regarding the information security and safety of their customers, partners and suppliers and therefore, they need to face a wide set of cyber specific challenges.

Based on the growing international linking of companies and especially of terminals as nodes in the global freight transport, the topic of IT security is gaining in importance. Although IT security plays an important role in the maritime supply chain environment, the modern methods of risk management have not paid a lot of attention to it so far.

Therefore since September 2015, thirteen partners from research and development, logistics and port administrations from Germany, Austria, Italy, Spain, United Kingdom, Greece and Romania developed the innovative Risk Management System MITIGATE, which intends to close this gap.



Exemplary Illustration of the Maritime Critical Information Infrastructure

MITIGATE at national and European events

The MITIGATE tool was presented at international fairs, scientific conferences, workshops and numerous other technical and business meetings.

The MITIGATE system was, among other events, presented at the transport logistic 2017 in Munich, the ARES-Conference 2017 in Reggio Calabria and at the “Security and Safety at the EU ports 2018” Conference in Piraeus (from the top)

PROTECTING MARITIME SUPPLY CHAIN IT INFRASTRUCTURE

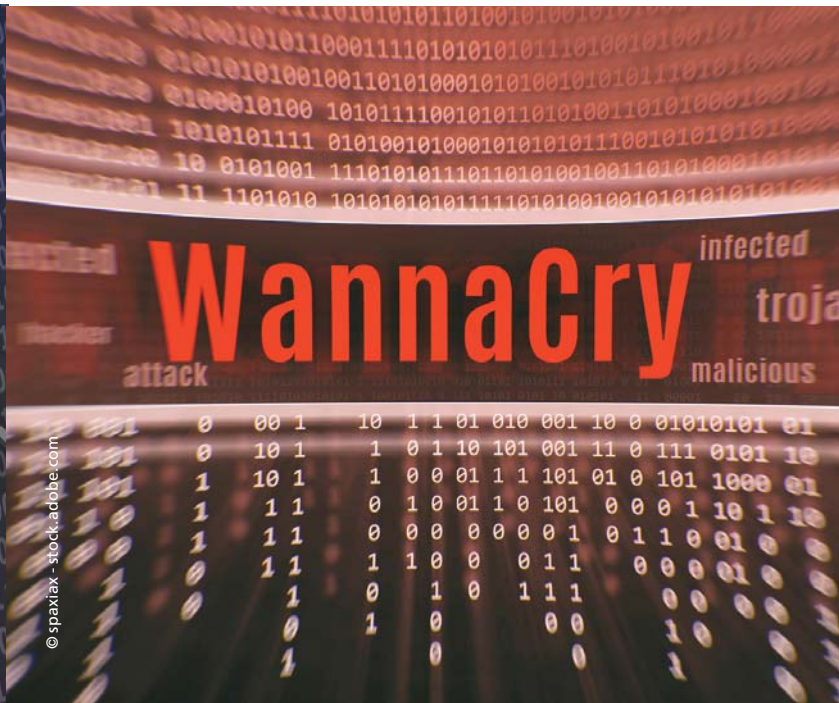
MEASURES AGAINST CYBER RISKS IN THE MARITIME SUPPLY CHAIN

Until recently, regulations on cyber security for ports and the maritime supply chain did not exist.

However, although not many cyber events have been reported, a number of incidents have revealed new threats in the last years. Cyber criminals have not only succeeded in shutting down or infecting software and hardware infrastructures, but also in diverting or misleading cargoes, ships and terminal equipment. Last but not least, pirates are using the digital world to obtain information about ships and cargoes.

Experts expect that the increasing networking of digital assets and Maritime 4.0 solutions will enable easier and more effective cyber attacks. A global study of risk experts ranked cyber incidents as the third highest business risk worldwide for all industries and expects it to be the highest business risk in the future.

This is why maritime organisations, classification societies and international administrations are setting standards to prevent the emergence and spread of cyber incidents. The risk assessment module of the MITIGATE system takes all these requirements into account.



PROTECTING MARITIME SUPPLY CHAIN IT INFRASTRUCTURE

BACKGROUND OF THE NOTION

Ports are considered critical infrastructures in the transport and traffic sectors because they act at the interface of information flows of many users in the globalised world. Their IT infrastructures are at risk with regard to cybercriminal assaults, as they increasingly have to provide access and data exchange of digital information due to the digitization of most of the relevant business processes.

In order to prevent malware from shutting down operations and to discourage data manipulation, a solution for identifying threats along the supply chain is urgently needed. For this reason, international and European as well as governmental institutions are demanding binding procedures and guidelines in order to be prepared for the new threats, and thus they are working intensively on their development and implementation.

In the EU-funded project MITIGATE, the project partners have created a software environment in which companies in the maritime supply chain can carry out a self-test of the hardware and software assets they use. This solution provides all companies and organizations in the maritime supply chain an easy-to-use, and, at the same time, effective risk management system that enables them to achieve timely detection of cyber threats.

"PROTECTION OF IT ASSETS" - OBSERVATIONS OF A PILOT USER

"In recent years there has been an ever-greater increase in different risk situations in ports that affect the organizations' communication systems labelled "cyber-attacks". This, along with the ever-more sophisticated development of information and communication technologies, has contributed to the exponential increase in virtual threats, which are no less dangerous for being intangible.

In this framework, MITIGATE provides the ports a "strategy" protection of information assets by addressing threats to information processed, stored, and transported by internetworked information systems."

Rafael Company, Security Project Manager at Valenciaport Foundation

PROTECTING MARITIME SUPPLY CHAIN IT INFRASTRUCTURE

CONSTRUCTING THE MITIGATE BACKBONE

The project started with the analysis of the requirements of the prospective users of the MITIGATE system. To this end, a questionnaire was developed and distributed to stakeholders, such as port authorities and port IT security managers.

Results from these questionnaires showed, that the stakeholders laid focus on an easy-to-use, but also collaborative solution.

To develop the MITIGATE system, a thorough review and selection of mathematical instruments and risk models, that could be integrated, followed. Concluding this step, the MITIGATE methodology was formulated, along with the architecture of the MITIGATE software system.

The next step in the project's course was the detailed specification of concepts, data structures, components and communication between the individual modules. The technical specifications defined in this step, including innovative concepts such as the use of game theory elements, provided the basis for the development of the MITIGATE system.

The integration and implementation of the MITIGATE system took place in the second half of 2016. The result was a risk management system specifically designed for the special needs of users of information infrastructures in the maritime supply chain.

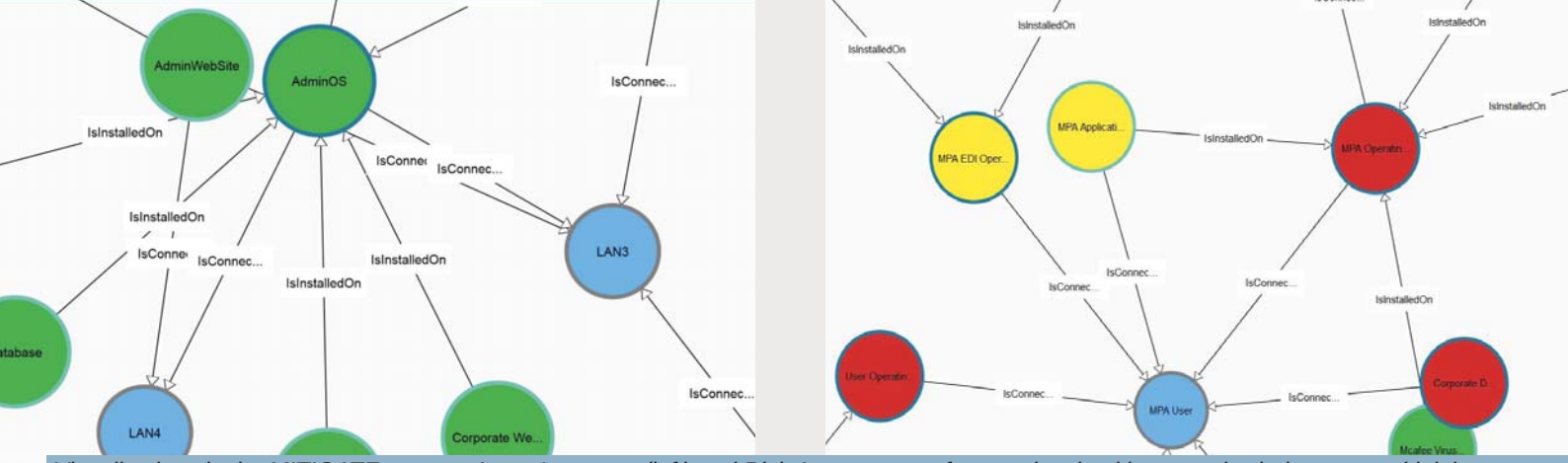
PROTECTING MARITIME SUPPLY CHAIN IT INFRASTRUCTURE

DEVELOPMENT AND TEST OF THE SYSTEM

In 2017, the cloud-based infrastructure was established, which supports the MITIGATE governance model, including the roles of the various stakeholders and their interactions with the system. Furthermore, the Open Intelligence and BigData Analytics module, used to realize the risk prediction and forecasting functionalities, was implemented.

To ensure proper tests and a thorough evaluation of the MITIGATE system, five pilot sites were chosen: the ports of Bremen/ Bremerhaven, Livorno, Ravenna, Piraeus and Valencia. In the preparation phase for the user tests, the representatives from these ports were trained to use the MITIGATE system. Furthermore, the ports and their dedicated supporting partners from the consortium developed plans to present the MITIGATE system to their business partners. Later on, the pilot operations spread from internal to external users. Experiences of the pilot users were gathered during the system's demonstrations and, more structured, through specific questionnaires. The analysis of these results was used to optimize the MITIGATE system for the dedicated user groups.

Finally, an intense evaluation methodology was developed to ensure the user-friendliness of the MITIGATE system from a stakeholder's perspective. Overall, the MITIGATE system reached the goals set.



Visualizations in the MITIGATE system: Asset Inventory (left) and Risk Assessment of assets involved in a supply chain process (right)

PROTECTING MARITIME SUPPLY CHAIN IT INFRASTRUCTURE

SETTING UP THE MITIGATE SYSTEM IN FIVE STEPS

1. BUILD AND MAINTAIN THE ASSET INVENTORY

All the IT assets involved in information exchange processes are described in the Asset Inventory. In order to do so, the user chooses names and descriptions for each asset and announces the asset type .
The MITIGATE Asset Editor and other existing data sources can be used in this process, but the use of a third party inventory tool might be more practical for big IT systems. All the assets and their relationships are depicted as a graph in the MITIGATE system (see left picture above).

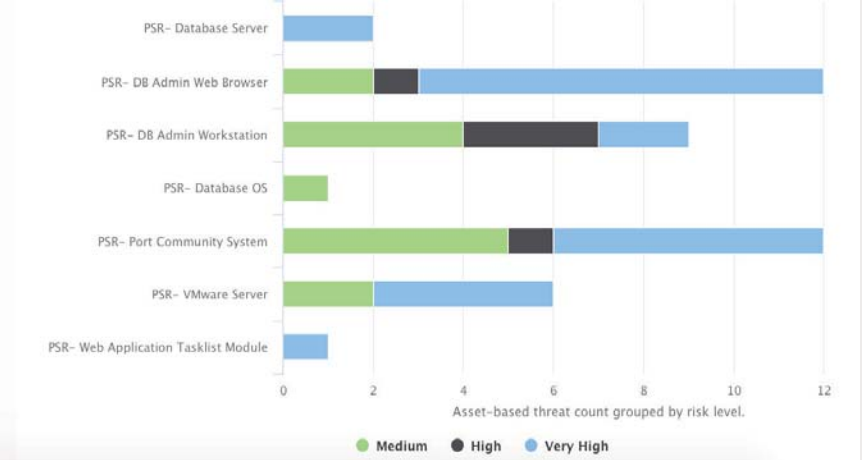
In this step, an innovative Vendor Management enables the user to provide information on assets that are tailormade and thus not included in the list that comes with the system. To do so, the name and other specific parameters concerning the vendor of an asset can be filled in in this section.

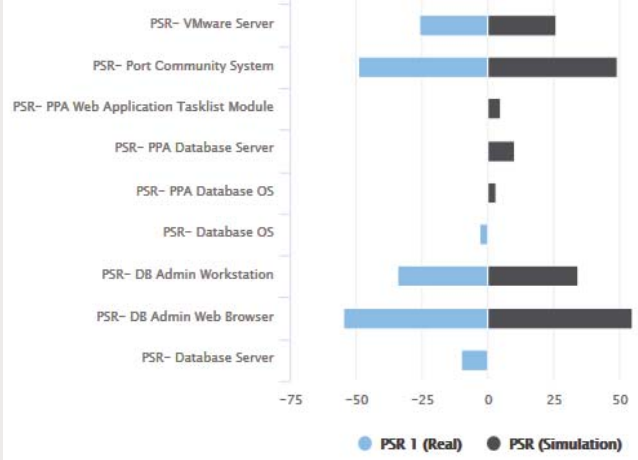
2. DEFINE SUPPLY CHAIN SERVICES AND PROCESSES

The Supply Chain Services and their supporting processes are created in this step by simulating the information flow. The picture above on the right shows the risk assessment of assets involved in a supply chain process. Colors show their specific risk levels: green for low, yellow for medium and red for very high risks of being vulnerable to cyber attacks.

3. COLLABORATE WITH BUSINESS PARTNERS

To integrate business partners into the risk assessment of a supply chain service, the initiator of a Supply Chain Service invites the involved partners to join the system. This can be done by using the Business Partners Management section. The partners receive invitations to join the system.





Screenshots from the MITIGATE system: Distribution of threats per asset (left) and Comparison of Risk Assessments (right)

PROTECTING MARITIME SUPPLY CHAIN IT INFRASTRUCTURE

SETTING UP THE MITIGATE SYSTEM IN FIVE STEPS

Thus, business partners are involved with their dedicated interfaces to the user's IT infrastructure. To achieve this, the initiator of a supply chain service defines the assets that serve as exchange points to the partners. Nevertheless, data security is ensured, so no partner in a supply chain can see another one's IT assets.

4. EXECUTE THE RISK ASSESSMENT

The outcome of the Risk Assessment shows the risk levels and threats for single assets and calculates the risk level of all assets involved. Diagrams and reports are the results on which the user can depend on (see left picture above), since the assessment is are based on international standards. The user of the MITIGATE system can run and compare (see right picture above) Risk Assessments for a supply chain process. This enables the user to analyze the influence of different controls or countermeasures. At the end, the most critical threats are illustrated for all involved assets.

5. DESIGN AND EVALUATE MITIGATION STRATEGIES

Before engaging in an action, a thorough Mitigation Strategy must be developed. As security controls and policies come with a price, a specific approach for evaluating different mitigation strategies is needed. The MITIGATE system offers the possibility to compare different mitigation scenarios. The user can calculate the residual risk of each strategy and compare it to the status quo. MITIGATE showcases the scenario with the minimal risk to provide assistance in the decision process.

PROTECTING MARITIME SUPPLY CHAIN IT INFRASTRUCTURE

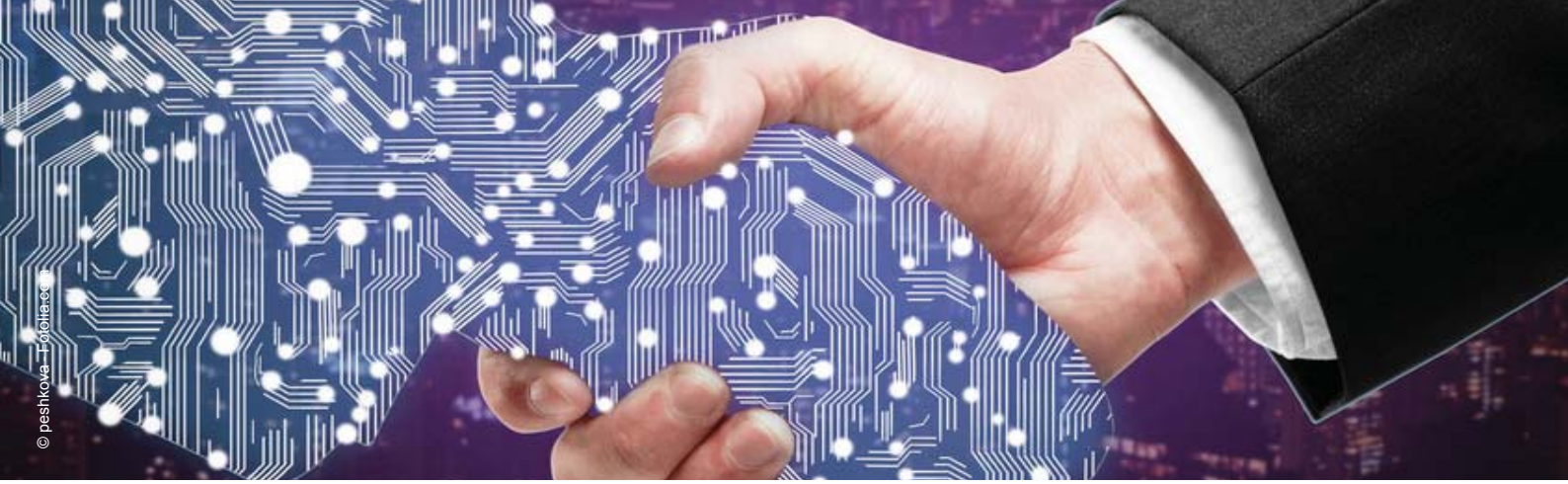
HARVEST INFORMATION FROM THE INTERNET

MITIGATE makes use of various innovative services, such as Social Engineering and Open Intelligence. The world wide web is full of cyber-security related content. Social media like Twitter and Reddit, as well as security blogs, RSS feeds and general-purpose websites, contain invaluable information about disclosed vulnerabilities, cyber threats, exploitation methods and security controls. The Open Intelligence module collects information from various sources, analyzes their content, classifies their relevance to the cyber-security sector and stores the results for further browsing and analysis. MITIGATE offers three different activities to make use of the gathered knowledge.

OPEN INTELLIGENCE SOURCE MANAGEMENT
The Open Intelligence Source Management provides data from resources such as social networks, blogs etc. The user selects the sources in which a search shall be conducted, and also adds or deletes sources to customize the search. Keywords make the search more specific and the results more concrete.

OPEN INTELLIGENCE NEWS PREVIEW
In this step, MITIGATE users can view cyber-security news relevant to their assets. The assets' dedicated identifier is used to define the relevance of a news entry with the business partner's asset inventory. Further searching is allowed via a wide set of available filters (e.g. time-range and free-text).

OPEN INTELLIGENCE NEWS SEARCH AND FILTERING
This item provides a functionality similar to the Open Intelligence News Preview. In contrast to the previous activities, the search here is independent of the assets used. In this way, a user can find out about reports on assets that he or she may plan to use later.



PROTECTING MARITIME SUPPLY CHAIN IT INFRASTRUCTURE

SELECTION OF THE RIGHT MITIGATION STRATEGY

MITIGATE provides several mitigation strategies. The strategy that fits the risk profile of the specific user can be evaluated by using the game theory module.

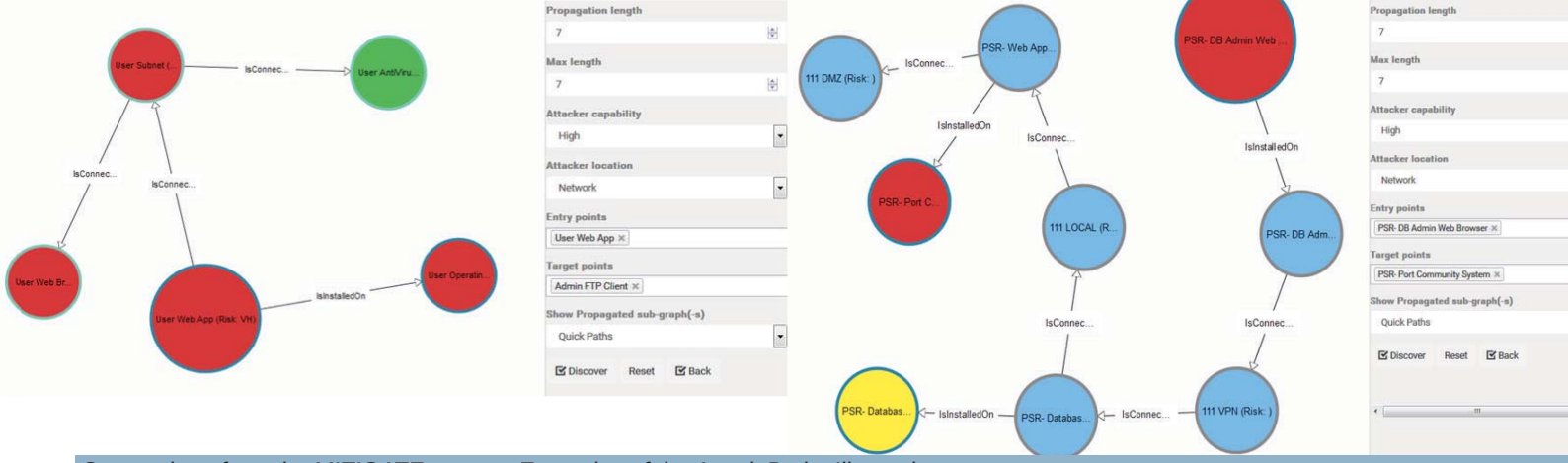
With the observation of comparable systems, but also of the behavior of users and attackers, weaknesses can be accurately and comprehensively eliminated. Specific game theoretic concepts and algorithms have been developed for use in the MITIGATE project.

The main idea is to model an attack on a company's ICT infrastructure as a game between the attacker and the system administrator. In this context, the attacker has a number of strategies at hand to infiltrate the infrastructure. Similarly, the system administrator has a number of defensive actions to counter these attacks. By evaluating the expected damage caused by an attack, game theory provides system administrators with an optimal defense strategy.

To this end, the expected damage needs to be estimated. Such an estimation can be achieved by collecting expert opinions and it can be further supported by a technical analysis of the system. In contrast to the classical game theory, the MITIGATE method does not condense the collected data, as it is done, when using the maximum principle, but it works with all the available information.

Game theoretical methods can be generalized to yield an optimal defense strategy, even in the situation of multiple security objectives. An equilibrium can be computed which is optimal under all security objectives. Furthermore, it is possible to prioritize different objectives by assigning weights.

Overall, the game theoretic approach offers completely new ways to protect critical information infrastructures since it provably provides optimal outcomes and efficiency. Furthermore, the application of this approach supports the dynamic and flexible evolution of the MITIGATE software.



Screenshots from the MITIGATE system: Examples of the Attack Paths Illustration

PROTECTING MARITIME SUPPLY CHAIN IT INFRASTRUCTURE

DISCOVERY OF ATTACK PATHS

Another special feature of the MITIGATE system is the identification of possible attack paths. A cyber-attack may not end at the first asset hit in a network, but use the possibility to spread through the network. Moreover, an attack may not stop at the borders of the attacked company's own network, but it may also infiltrate the connected networks of the company's business partners. One should also be aware that there might be unknown vulnerabilities which are hard to prepare against. In this case, the knowledge of the connected network is invaluable. If the structure and composition of a network are known, it might be possible to stop an attack before the damage spreads, resulting in a cascading effect.

The MITIGATE system includes an algorithm to discover attack paths. In particular, it examines how an attacker can exploit identified cyber asset vulnerabilities in order to perform malicious actions. The pictures above show possible attack paths, that enable a highly skilled attacker to exploit the target points.

To set up an attack path scenario, the user must estimate the attacker's capability, entry and target points of the attack and possible lengths of the attack (number of assets that can be exploited on the path through the networks).

Attack paths (see pictures above) are then modeled by the system. The colours show the specific threat levels of the connected assets (red: very high, yellow: high, blue: medium and green: low). In this way, the user can analyse how to increase the overall security level by securing important assets, which may have a minor importance for the network functionality, but act e.g. as gatekeepers.

It should be noted, though, that the attack path functionality needs specific input. The algorithm requires a detailed physical network topology, consisting of cyber assets and their relationships, an asset configuration, and a set of entry points and target points.

PROTECTING MARITIME SUPPLY CHAIN IT INFRASTRUCTURE

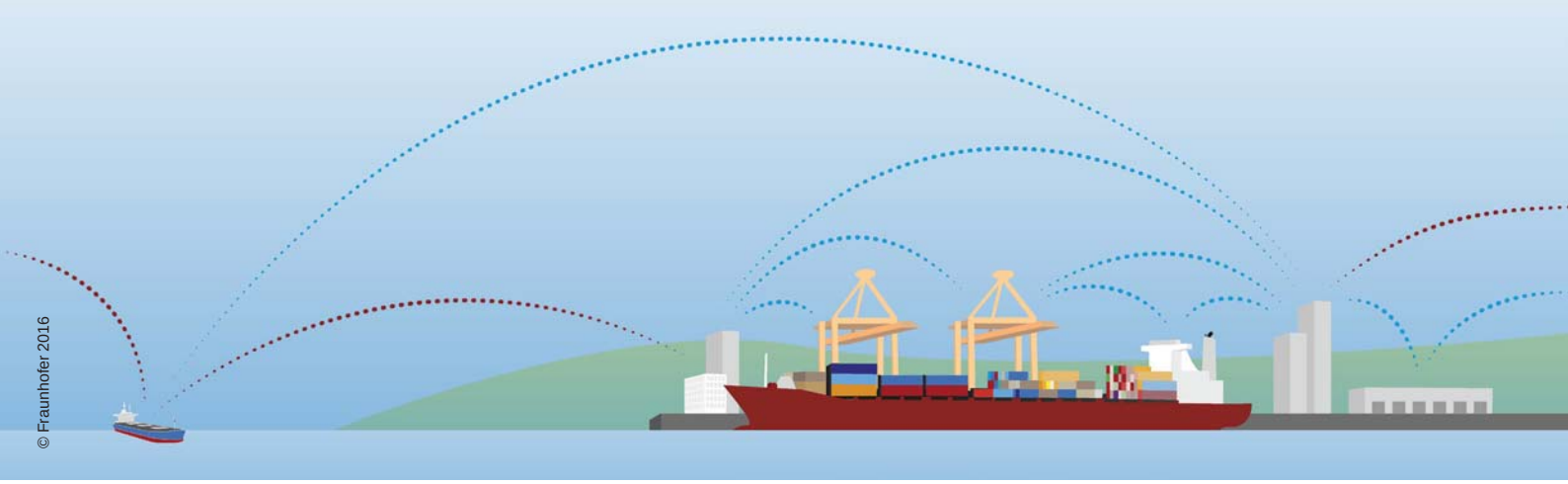
"IMPROVING LEVELS OF SECURITY" - OBSERVATIONS OF A PILOT USER

"During the last years it became more and more obvious that our ports are no lucky islands in the IT landscape any more. We had to learn that organized criminals had entered into port IT systems or had misused terminal IT devices using internal support. The maritime community was shocked last year when malware NotPetya did affect a major maritime player among many other companies from all over the world, when terminals had been out of order for several days and some most modern ones had been hit worst.

We have to think about our ports´ resilience against a comprehensive cyber attack. Pilots will be able to do their job without IT, if ships will stay maneuverable. Will they stay? Fire brigade will arrive without IT, if the alarming system will run. Vessel traffic control might still work in our ports as we can communicate via VHF and as long as we fix information status on white boards. But is VHF still VHF in times of digital radio communication?

MITIGATE could help us to do our IT inventory and to give us an overview over our IT relationships. It could point out possible risky "attack paths" and by comparing simulations we could look for suitable solutions to mitigate risks in most economical or most effective ways. Furthermore, MITIGATE could be a challenge for cooperation in our business. Improving levels of security could be achieved along the supply chain if business partners would share a common risk assessment tool, without being forced to disclose their internal IT structure to their partners."

Dieter Hentschel, security officer at the harbourmaster´s office in the ports of Bremerhaven/ Bremen, Germany



PROTECTING MARITIME SUPPLY CHAIN IT INFRASTRUCTURE

PARTNERS

Fraunhofer CML
Gruppo Maggioli
University of Piraeus Research Center
FEPORTS – Instituto Portuario de Estudios y Cooperación de la Comunitat Valenciana
SingularLogic – Innovation at your doorstep
IMSSEA
University of Brighton
OAΠ – Piraeus Port Authority S.A.
AIT Austrian Institute of Technology
Port of Ravenna Authority
dbh Logistics IT AG
Fundación Valenciaport
Autorità portuale Livorno
Hansestadt Bremisches Hafenamt

KEY FIGURES

- Thirteen partners from research, software development, logistics and ports
- Partners‘ countries: Austria, United Kingdom, Germany, Greece, Italy, Romania and Spain
- Project duration: from September 2015 til February 2018
- Budget 3.5 m€, funded within the EU Horizon 2020 programme with 3.1 m€

This project has received funding from The European Union´s Horizon 2020 research and innovation programme under grant agreement No 653212.

PROJECT COORDINATION

Fraunhofer Center for Maritime Logistics and Services CML, Hamburg

TECHNICAL MANAGEMENT

University of Piraeus Research Center, Piraeus

CONTACT

info@mitigateproject.eu

MITIGATE
www.mitigateproject.eu

LinkedIn
www.linkedin.com/grps/MITIGATE-8472607

twitter.com/MITIGATE_EU